Background

Identify computers that are running operating systems that have reached end-of-life, and therefore does not receive new updates, leaving them vulnerable if vulnerabilities are found.

There are two attributes that are of relevance here:

```
operatingsystem             - show you the OS version, Windows Server 2008 for example
operatingsystemversion      - it stores the version of the OS.
```

Can these attributes be trusted?

Yes and no. They are updates when a domain computer is joined, and when updated and restarted. So in that sense it should be fairly up to date. But it can be changed manually on the computer.

"AD relies on the individual Windows computers to take care of it – such as when joining the domain, being upgraded, being service packed, or after reboot."

https://docs.microsoft.com/en-us/archive/blogs/askds/monthly-mail-sack-i-hope-your-data-plan-is-paid-up-edition#ados

Pre-requisites

Domain account.

Risks

No risks.

How to check for

In bloodhound the following query can be made:

```
MATCH (H:Computer {enabled: true}) WHERE H.operatingsystem =~ '(?i).*(2000|2003|2008|xp|vista|me).*' RETURN H.name,H.operatingsyster
```

How to exploit

Recommendation

Related Vulnerabilities

- vuln_

References

https://docs.microsoft.com/en-us/archive/blogs/askds/monthly-mail-sack-i-hope-your-data-plan-is-paid-up-edition#ados